



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/943,405	08/30/2001	Robert P. Goldman	H0001867 (FSP:114.001US01)	8248
7590 05/09/2007 Honeywell International Inc. Law Dept. AB2 P.O. Box 2245 Morristown, NJ 07962-9806			EXAMINER SHERKAT, AREZOO	
			ART UNIT 2131	PAPER NUMBER
			MAIL DATE 05/09/2007	DELIVERY MODE PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

# Office Action Summary

Application No.

09/943,405

Applicant(s)

GOLDMAN ET AL.

Examiner

Arezoo Sherkat

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

- 1) ☒ Responsive to communication(s) filed on 29 January 2007.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

- 4) ☒ Claim(s) 1-20 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-20 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

## Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

## Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: \_\_\_\_\_

***Response to Amendment***

This office action is responsive to Applicant's amendment received on 1/29/2007. Claims 1-10 and 17 have been amended. Claims 1-20 remain pending.

***Claim Rejections - 35 USC § 101***

In light of the amendment received on 1/29/2007, the rejections of claims 1-3 and 4-10 have been withdrawn.

***Claim Rejections - 35 USC § 112***

In light of the amendment received on 1/29/2007, the rejections of claims 1-10 have been withdrawn.

***Response to Arguments***

Applicant's arguments filed 1/29/2007 have been fully considered but they are not persuasive.

Regarding claims 11-20, Applicant argues that "Rothermel's Security Policy Manager Device 110 is not a "database engine" (Remarks, page 11).

Examiner responds that Rothermel's Security Policy Manager Device Management system does include generating a security policy template containing of security policy filter rules. As an example, security policy rule 301 specifies/deduces that the outgoing FTP connections are allowed only from network elements defined as being within the "Information Services" alias (col. 4, lines 30-49 and col. 8, lines 8-35).

Applicant further argues that substitution of pre-defined values for variables in a template does teach Applicants' claimed step of "using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device" (Remarks, page 11).

Examiner responds that Rothermel's Security Policy Management System has "A security template 300 is first generated, such as by a user of the manager device. Then, for each of a number of different networks 315, 325, 335, etc., the user generates a network profile containing NSD-specific information for implementation by the NSD protecting that network. These network profiles are shown as network profiles 310, 320, 330, etc. In order to generate the specific security policy for each network, the security policy template is combined with the network profile for that network (i.e., using active inference in a database engine to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device – wherein a class of network devices/a network profile contains a definition of a "Information Services" alias, including network elements with a specific IP addresses). For example, in order to create security policy 315 for network 1, the security policy template 300 is combined with network profile 310 for network 1 (col. 10, lines 8-65).

Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references.

***Claim Rejections - 35 USC § 102***

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

Claims 1, 11-12, and 17-20 are rejected under 35 U.S.C. 102(e) as being anticipated by Rothermel et al., (U.S. Patent No. 6,678,827 and Rothermel hereinafter).

Regarding claim 1, Rothermel discloses a system for configuring security software on a computer network (col. 5, lines 14-27), the system comprising:

a database engine providing deduction (i.e., Security Policy Manager Device Management system does include generating a security policy template containing of security policy filter rules. As an example, security policy rule 301 specifies/deduces that the outgoing FTP connections are allowed only from network elements defined as being

within the "Information Services" alias)(col. 10, lines 8-35), a network information database associated with the database engine and providing a central repository for a configuration of hardware and software installed on the network (i.e., network security information log 125 and 165)(col. 7, lines 57-67 and col. 8, lines 1-7), and a security goal database associated with the database engine and describing uses that the hardware and software installed on the network are permitted to support (i.e., security policy information 116)(col. 7, lines 3-15).

Regarding claim 11, Rothermel discloses a method for configuring a security software package installed on an individual network device, the method comprising:

using active inference in a database engine (i.e., security policy manager device – Fig. 1) to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device (col. 10, lines 44-65), wherein the individual network device is a member of the class of network devices (i.e., external, optional, and trusted devices based on defined networks: network 1, network 2, ...)(col. 6, lines 20-32); and

configuring the security software package (i.e., security device software 132 and 142) using the one or more security goals (i.e., NSD's specific security information)(col. 7, lines 3-56).

Regarding claim 12, Rothermel discloses the method of claim 11, wherein using active inference further comprises automatically classifying the individual network

Art Unit: 2131

device based on an IP address (col. 11, lines 62-67 and col. 12, lines 1-10), a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification (col. 10, lines 65-67 and col. 11, lines 1-45).

Regarding claims 17, Rothermel discloses a method for configuring a security software package, the method comprising:

defining one or more security policies for a class of network devices (i.e., security policy templates can be viewed as defining levels of trust given to various specific devices or classes of devices), wherein the security software package is a service running on at least one network device of the class of network devices (i.e., security device software 132 and 142)(col. 6, lines 20-32);

using a database engine (i.e., security policy manger device – Fig. 1) providing deduction to decompose the one or more security policies for the class of network devices into one or more security goals, using a database engine providing deduction to associate the one or more security goals with the at least one network device (i.e., combining the security policy template 300 with the network profile 310 for network 1 to create the security policy 315 for network 1)(col. 10, lines 24-65); and

configuring the security software package (i.e., security device software 132 and 142) on the at least one network device using the one or more security goals (i.e., NSD's specific security information)(col. 7, lines 3-56).

Regarding claim 18, Rothermel discloses a method for configuring security software packages, comprising:

generating a first database containing a configuration of hardware devices and software packages installed on a network (i.e., security policy templates - element 113 on storage 11), wherein the software packages include the security software packages (col. 6, lines 54-67);

defining classes of hardware devices installed on the network (i.e., security policy templates can be viewed as defining levels of trust given to various specific devices or classes of devices), automatically classifying each of the hardware devices into one of the classes of hardware devices using a database engine (i.e., security policy manager device 110) providing deduction (col. 6, lines 7-54);

generating a second database (i.e., network security information log) containing first security goals (col. 7, lines 57-67 and col. 8, lines 1-27);

decomposing the first security goals (i.e., security policy templates) into second security goals (i.e., NDS-specific security policy information) for individual hardware devices using the database engine and the configuration of the hardware devices and the software packages installed on the network (col. 10, lines 8-24); and

configuring the security software package (i.e., security device software 132 and 142) on the at least one network device using the second security goals (i.e., NSD's specific security information)(col. 7, lines 3-56).



Regarding claim 19, Rothermel discloses wherein generating a second database containing first security goals further comprises generating a second database containing first security goals for each class of hardware devices (i.e., network profiles)(col. 7, lines 57-67 and col. 8, lines 1-27).

Regarding claim 20, Rothermel discloses the method of claim 19 wherein decomposing the first security goals for individual hardware devices further comprises using inference to associate the second security goals with individual hardware devices within each class of hardware devices (i.e., the rules in security policy 315 for network 1, which are to be implemented in network 1, specifically refer to network elements within network 1. In this sense, they differ from the rules in security policies 325 and 335, which specifically refer to network elements within networks 2 and 3, respectively)(col. 10, lines 8-24).

### ***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 2-10 and 13-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rothermel et al., (U.S. Patent No. 6,678,827 and Rothermel

hereinafter), in view of Schneier et al., (U.S. Publication No. 2002/0087882 and Schneier hereinafter).

Regarding claims 4 and 10, Rothermel discloses a configuration tool implemented on a computer-readable medium for use in configuring security software packages on a computer network, the configuration tool comprising:

a description logic database engine (i.e., Security Policy Manager Device Management system does include generating a security policy template containing of security policy filter rules. As an example, security policy rule 301 specifies/deduces that the outgoing FTP connections are allowed only from network elements defined as being within the "Information Services" alias)(col. 10, lines 8-35);

a network information database associated with the description logic database engine and providing a central repository for a configuration of hardware and software installed on the network (i.e., network security information log 125 and 165)(col. 7, lines 57-67 and col. 8, lines 1-7);

a security goal database associated with the description logic database engine and providing security goals describing uses that the hardware and software of the network are permitted to support (i.e., security policy information 116)(col. 7, lines 3-15);

Rothermel further discloses updating some or all of the software components used by the NSDs (i.e., such as intrusion detection and blocking software)(col. 7, lines 39-56), and allowing control for incoming and outgoing packets based on specific

senders and recipients and based on specific security policy information (col. 11, lines 1-17).

a first configuration module coupled to the description logic database engine (i.e., a first software component) [for configuring intrusion blocking security software packages], and a second configuration module coupled to the description logic database engine (i.e., a second software component) [for configuring intrusion detecting security software packages], wherein the first configuration module configures the intrusion blocking security software packages based on the configuration of the hardware and software installed on the network and the security goals, and wherein the second configuration module configures the intrusion detecting security software packages based on the configuration of the hardware and software installed on the network and the security goals (i.e., wherein security device software 132 and 142 are intrusion detection and intrusion blocking software packages)(col. 7, lines 39-56).

Schneier further discloses updating customer software, including antivirus signature files and software, firewall software, and router software (par. 35-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include updating customer software, including antivirus signature files and software, firewall software, and router software as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of

predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage and implement rapid refinement necessary to combat network attacks (Schneier, par. 7-8).

Regarding claim 15, Rothermel discloses a method for configuring a security software package installed on an individual network device, the method comprising:  
using active inference in an object-oriented description logic database engine (i.e., security policy manger device – Fig. 1) to decompose one or more security policies for a class of network devices into one or more security goals for the individual network device (col. 10, lines 44-65), wherein the individual network device is a member of the class of network devices(i.e., external, optional, and trusted devices)(col. 6, lines 20-32); and

configuring the security software package using the one or more security goals, wherein the security software package is selected from the group [consisting of an intrusion blocking software package and an intrusion detecting software package] (col. 7, lines 25-56).

Schneier further discloses updating customer software, including antivirus signature files and software, firewall software, and router software (par. 35-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include updating customer software, including antivirus signature files and software, firewall software, and router software as

Art Unit: 2131

disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage and implement rapid refinement necessary to combat network attacks (Schneier, par. 7-8).

Regarding claim 2, Rothermel discloses the system of claim 1. Rothermel does not disclose an event database containing events related to the network, after probing the network for vulnerabilities.

However, Schneier discloses a network intrusion monitoring, detection, and response system, further comprising:

an event database (i.e., problem/event database) associated with the database engine and containing events related to the network, wherein such events include benign network events, suspected network attacks, and actual network attacks (par. 85-86).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include an event database containing events related to the network as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident

according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage (Schneier, par. 7).

Regarding claim 3, Rothermel discloses the system of claim 1. Rothermel further provides a GUI for viewing and modifying the existing security policy, which may be implemented in an object-oriented language such as Java (col. 12, lines 14-67 and col. 13, lines 1-20).

However, Schneier discloses wherein the database engine is an object-oriented description logic database engine (par. 59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include wherein the database engine is an object-oriented description logic database engine as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier for easy porting to a wide variety of hardware or be based on certain preexisting commercially available software (Schneier, par. 59).

Regarding claim 5, Rothermel and Schneier disclose the configuration tool implemented on a computer-readable medium of claim 4. Schneier further comprising:

an event database (i.e., problem /event database) associated with the description logic database engine and containing events related to the network (par. 85-86).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include an event database containing events related to the network as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage (Schneier, par. 7).

Regarding claim 6, Rothermel and Schneier disclose the configuration tool implemented on a computer-readable medium of claim 5. Schneier further discloses wherein the events contained in the event database includes benign network events, suspected network attacks, and actual network attacks (i.e., events or incidents)(par. 35-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include an event database containing events related to the network as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and

shut down the vulnerability before the attacker does any damage and to allow for customization and complex data analysis (Schneier, par. 7 and 8).

Regarding claim 7, Rothermel and Schneier disclose the configuration tool implemented on a computer-readable medium of claim 4. Schneier discloses further comprising:

a system-hardening module coupled to the description logic database engine for automating a process of hardening the network (i.e., mitigating a detected attack)(par. 7-8 and par. 68).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include a system-hardening module coupled to the description logic database engine for automating a process of hardening the network as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage and implement rapid refinement necessary to combat network attacks (Schneier, par. 7-8).



Regarding claim 8, Rothermel and Schneier disclose the configuration tool implemented on a computer-readable medium of claim 7. Schneier further discloses wherein the system-hardening module is context sensitive (par. 7-8).

Regarding claim 9, Rothermel and Schneier disclose the configuration tool implemented on a computer-readable medium of claim 4. Schneier discloses further comprising: an audit configuration module coupled to the description logic database engine for probing the network for vulnerabilities (par. 7-8 and par. 35-38).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include a system-hardening module coupled to the description logic database engine for probing the network for vulnerabilities as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage and implement rapid refinement necessary to combat network attacks (Schneier, par. 7-8).

Regarding claim 13, Rothermel discloses the method of claim 11. Rothermel further provides a GUI for viewing and modifying the existing security policy, which may

be implemented in an object-oriented programming language such as JAVA (col. 12, lines 14-67 and col. 13, lines 1-20).

However, Schneier discloses wherein the database engine is an object-oriented description logic database engine (par. 59).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include wherein the database engine is an object-oriented description logic database engine as disclosed by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier for easy porting to a wide variety of hardware or be based on certain preexisting commercially available software (Schneier, par. 59).

Regarding claim 14, Rothermel discloses the method of claim 11. Rothermel does not explicitly disclose wherein the security software package is selected from the group consisting of an intrusion blocking software package an intrusion detecting software package.

However, Schneier discloses updating customer software, including antivirus signature files and software, firewall software, and router software (par. 35-37).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Rothermel with teachings of Schneier because it would allow to include updating customer software, including antivirus signature files and software, firewall software, and router software as disclosed

Art Unit: 2131

by Schneier. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Schneier to provide the capability to escalate the handling of the incident according to a variety of predetermined escalation procedures to stop the attack and shut down the vulnerability before the attacker does any damage and implement rapid refinement necessary to combat network attacks (Schneier, par. 7-8).

Regarding claim 16, Rothermel discloses the method of claim 15, wherein using active inference further comprises automatically classifying the individual network device based on an IP address (col. 11, lines 62-67 and col. 12, lines 1-10), a network topology and one or more services the individual network device provides, and applying rules to the individual network device based on its classification (col. 10, lines 65-67 and col. 11, lines 1-45).

### ***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Please refer to the attached PTO-892 for a detailed listing.

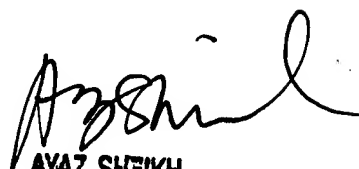
Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.

Art Unit: 2131

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.  
Patent Examiner  
Group 2131  
April 29, 2007

  
AYAZ SHEIKH  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100